di Manlio Cammarata

L'autoregolamentazione per gli Internet provider

Un codice di regole per la libertà della Rete

E' in fase di elaborazione un insieme di norme di comportamento per i fornitori di servizi telematici. Deve essere rivolto soprattutto alla protezione dei diritti dell'utente e deve assicurare ai provider la certezza di operare nei limiti della legge, con diritti e doveri ben definiti.

"Internet, se la conosci la eviti", ha detto qualcuno non molto tempo fa. Un mondo senza leggi, popolato di malfattori, terroristi, maniaci sessuali. Un Far-West dove "si corre persino il rischio di essere uccisi", come abbiamo letto su un periodico dei giornalisti, citato in queste pagine su MCmicrocomputer n. 165 (settembre '96). Un fatto è certo e capovolge lo slogan: "Internet, se non la conosci la eviti". Perché chi conosce Internet sa bene che i contenuti illegali, o comunque discutibili, sono una percentuale piccolissima delle informazioni che possono essere ricevute da decine di milioni di utenti. Solo chi non ha passato qualche ora "navigando" tra i link può pensare che il solo fatto di avere un accesso alla Rete possa mettere a repentaglio la salute mentale dei ragazzi, o trasformare una signorina per bene in una donna di malaffare.

Ma la pessima fama del "ciberspazio" continua a essere alimentata dai mass media, che in questo modo fanno il gioco di quanti, con il motivo o il pretesto di "regolamentare Internet", cercano in ogni modo di imporre sui contenuti della Rete qualche forma di censura, più o meno stretta e variamente mascherata. Si ribella il "popolo telematico": Internet è la dimostrazione di come la libertà di organizzarsi e di esprimersi favorisca la conoscenza, i rapporti tra gli individui, aiuti a costruire un mondo migliore. Nessuna censura, anzi nessuna regola, perché solo l'assoluta libertà ha determinato lo sviluppo di Internet come strumento di comunicazione universale.

Ma anche questa affermazione è falsa. Lo sviluppo della Rete non è avvenuto in assenza di regole, ma "al di fuori di regole imposte dall'esterno". Le regole ci sono state fin dall'inizio, e sono state norme tecniche e codici di comportamento. Il punto essenziale è che queste regole sono state accettate da tutti come presupposto dell'appartenenza alla comunità telematica. Sul piano tecnico l'adesione alle norme è connaturata alla possibilità di connettersi: chi non adotta i protocolli di Internet non può farne parte. Sul piano dei comportamenti il discorso è diverso, le regole operano come forme di autodifesa di un organismo vitale. O, meglio, hanno operato fino a quando Internet è stata soprattutto la rete mondiale della ricerca, cioè fino a quando i suoi "adepti" hanno potuto riconoscersi in una comunità, che poteva emarginare o espellere i soggetti che non si comportavano secondo le regole.

La situazione è cambiata. Oggi gli utenti di Internet appartengono a tutte le categorie, le professioni, le culture. Non costituiscono più un gruppo sostanzialmente omogeneo, ed è quindi venuta a mancare quella forma di adesione spontanea a valori condivisi che costituiva il "collante sociale" della Rete delle origini. Ormai l'aspetto economico prevale su quello culturale, Internet non è più "un mondo a parte", ma una parte del mondo di tutti. E riflette, fatalmente, gli aspetti positivi e negativi di questo mondo, compresi i comportamenti illegali o comunque discutibili.

Una legge "interna"

"Comportamenti illegali o comunque discutibili": torneremo più avanti su questa espressione. Ora è necessario ricordare che quando sulla Rete si parla di "comportamenti" ci si riferisce soprattutto alla diffusione di informazione e, in secondo luogo, alla commissione di fatti qualificabili come reati o contrari all'etica della Rete stessa. Quindi l'obiettivo è controllare e sanzionare la diffusione di determinati tipi di informazioni o eventuali azioni illegali o scorrette.

Fino a questo punto è difficile non essere d'accor-

do. I problemi incominciano quando ci si pone il problema di controllare, e se del caso punire, i comportamenti scorretti: chi stabilisce quali contenuti o quali comportamenti devono essere controllati, chi e come deve controllare e via discorrendo. I sostenitori della libertà incondizionata affermano che qualsiasi intervento normativo che provenga dall'esterno si risolve comunque in una forma di censura, intesa come limitazione della libertà di espressione. Si ribatte che nei paesi democratici ci sono leggi che nello stesso tempo proteggono la libertà di espressione e difendono dai comportamenti illeciti, con regole ormai collaudate. Chi ha ragione?
Il fatto è che Internet non è un mezzo di comunicazione come gli altri. La libertà di espressione che lo caratterizza non può essere difesa con semplici strumenti repressivi dei contenuti illeciti, perché la massa delle informazioni è incontrollabile dall'esterno senza mettere in piedi un poderoso apparato censorio. Ha ragione, a mio avviso, chi afferma che qualsiasi controllo esterno dei contenuti della Rete si può risolvere in una forma di censura. Ma in ogni caso è necessario che la diffusione di certi contenuti sia regolata, che i comportamenti illeciti siano puniti. La soluzione non può essere che all'interno del sistema, sulla base di norme accettate da tutti i soggetti coinvolti, come condizione per l'appartenenza al sistema stesso. Cioè con la sottoscrizione esplicita di un codice di autoregolamentazione vincolante, che offra "all'esterno" la garanzia che la diffusione dei contenuti avviene secondo principi di rispetto della libertà di tutti. E qui la libertà è intesa nel suo senso più ampio, non solo come libertà di comunica-

L'Unione Europea è al lavoro per la regolamentazione di Internet. Il rapporto alla Commissione è alla URL http://www2.echo.lu/legal/internet.html.

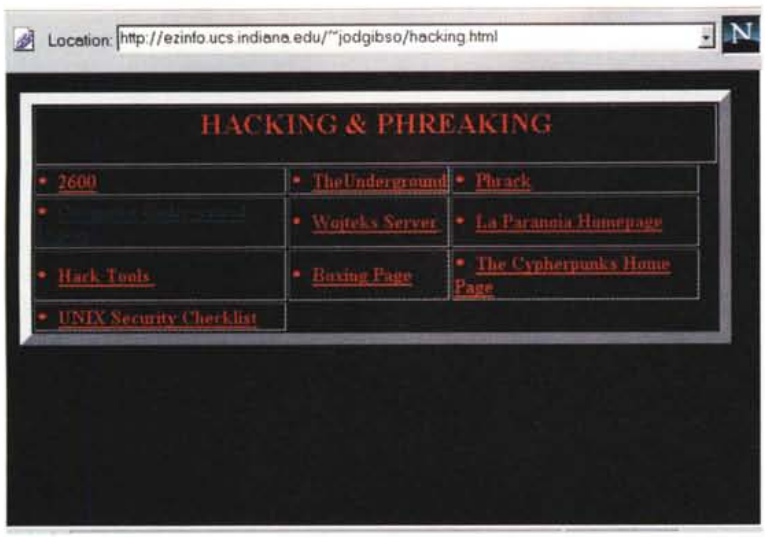
Bozza del codice di autoregolamentazione dei fornitori di servizi telematici

di Manlio Cammarata e Andrea Monti

Questo testo è parte di uno studio svolto nell'ambito del Forum multimediale LA SOCIETÀ DELL'INFORMAZIONE ed è stato comunicato al Ministero di grazia e giustizia come contributo alla definizione dei decreti legislativi previsti dalla legge-delega 676/96 sulla protezione dei dati personali. Non è una proposta definitiva, ma solo una bozza in fase di ulteriore elaborazione, che ha lo scopo di chiarire i punti più importanti dell'autoregolamentazione di Internet e delle attività telematiche in generale. Lo studio, dal quale sono stati tratti alcuni passaggi dell'articolo pubblicato in queste pagine, è alla URL http://www.mclink.it.it/inforum.

Premessa

Lo sviluppo delle attività telematiche, e in particolare di Internet, costituisce un punto di svolta fondamentale nello sviluppo della società. Per la prima volta nella storia l'uomo dispone di strumenti di dialogo e di conoscenza che annullano tempi e distanze fisiche, sociali e culturali. Lo sviluppo dell'economia vede ormai al primo posto, a livello mondiale, il fatturato delle attività legate alle tecnologie dell'informazione. Siamo dunque entrati in pieno in quella che chiamiamo "società dell'informazione".
Ma l'evoluzione presenta anche aspetti negativi. Già oggi ci sono forti differenze nelle opportunità di relazioni umane, di lavoro e di svago tra chi ha la possibilità di servirsi degli strumenti telematici e chi non le ha. Queste differenze sono destinate ad accentuarsi nel prossimo futuro, fino a far te-



Quando si parla di contenuti illegali su Internet: questo sito contiene una quantità di istruzioni ad uso dei pirati telematici: libertà di espressione o istigazione a delinquere?

zione, ma anche come protezione contro informazioni offensive o comportamenti illegali, come difesa della riservatezza degli individui e così via.
Un codice di autoregolamentazione deve prevedere anche un complesso equilibrato di sanzioni per i soggetti che non ne rispettino le regole. Questa è la condizione che ne rende possibile l'accettazione all'esterno e che di conseguenza allontana la possibilità che dall'esterno arrivino le regole. In altri termini, l'autoregolamentazione esorcizza lo spettro della censura. C'è un'ulteriore condizione essenziale: che la validità del codice "interno" sia riconosciuta "dall'esterno", cioè dall'ordinamento giuridico, dalla legge. E questo può rendere necessaria l'emanazione di leggi che sanciscano l'efficacia dell'autoregolamentazione, anzi, che ne costituiscano il presupposto.

Nocivo o pericoloso?

La maggior parte degli esperti ritiene che l'autoregolamentazione di Internet (e delle attività telematiche in generale) sia la strada migliore per assicurare il giusto equilibrio tra la necessità di proteggere i cittadini dai contenuti illegali o comunque discutibili e la libertà di comunicazione (per inciso: preferisco usare l'espressione "libertà di comunicazione" invece che "libertà di espressione", perché con la seconda formula si indica solo l'aspetto attivo dell'informazione, mentre con il termine mere una divisione della società in due classi: gli "info-ricchi" e gli "info-poveri". Un altro problema della società dell'informazione è costituito dalla diffusione sulle reti telematiche di contenuti illegali e pericolosi. Anche se essi rappresentano di fatto una percentuale bassissima delle informazioni disponibili, è necessario fornire alle autorità gli strumenti per la repressione dei reati e ai gruppi sociali e ai singoli individui gli strumenti per la selezione dei contenuti potenzialmente offensivi.
Terzo, ma non ultimo aspetto da considerare, è l'impossibilità di realizzare una regolamentazione efficace al di fuori di un concerto internazionale. Le reti telematiche costituiscono una specie di "meta-territorio" nel quale è difficile applicare singoli e non coerenti sistemi di leggi nazionali. Questo Codice si propone di favorire un corretto sviluppo delle attività telematiche in Italia, assicurando la libertà di lavoro e di espressione di tutti i soggetti interessati.
Tuttavia esso non può ottenere risultati significativi in assenza di un quadro legislativo chiaro e coerente, concordato a livello internazionale.

Titolo I – Generalità

1. Finalità
Il codice ha lo scopo di assicurare che l'offerta dei servizi di accesso alle reti telematiche comunque ed eventualmente interconnesse, e dei servizi di informazione a distanza avvenga secondo criteri di legalità e trasparenza, con particolare riferimento al rispetto dei diritti dell'utente finale.
Il codice individua e sanziona prassi e comportamenti che, pur conformi alla legge, contrastano con le sue finalità.
Il codice costituisce la fonte principale per l'autoregolamentazione.

2. Soggetti vincolati
Il codice vincola tutti coloro che, operando a qualsiasi titolo nel settore della telematica in Italia, vi aderiscono direttamente o per il tramite degli enti o delle associazioni o di altri organismi collettivi dei quali eventualmente facessero parte.

3. Obblighi degli aderenti
Gli enti e le associazioni e/o gli organismi collettivi che, in rappresentanza di singoli e/o di altre strutture, aderiscono al codice si obbligano a far accettare senza ritardo agli associati o aderenti i contenuti del codice stesso.
Gli stessi soggetti controllano che i singoli membri abbiano adottato senza ritardo le prescrizioni del Codice. Gli altri soggetti, persone fisiche o società di persone e/o di capitali, che aderiscono in proprio, adottano senza ritardo tutte le prescrizioni contenute nel codice.

4. Definizioni
Agli effetti del presente codice si intende per:
a) RETE TELEMATICA: una serie di almeno due computer comunque collegati fra di loro, a prescindere dalla permanenza della connessione, comunque raggiungibili dall'esterno.
b) SISTEMA TELEMATICO STAND-ALONE: il computer non connesso ad altri computer, in qualsiasi modo raggiungibile dall'esterno.
c) CARRIER SUPPLIER (CS): chiunque offre a terzi connettività dedicata.

"comunicazione" si sottolinea la bidirezionalità, il dare e il ricevere informazioni).
Ma quale deve essere il fine ultimo dell'autoregolamentazione? Secondo l'opinione più diffusa, accolta e propugnata anche in sede europea, lo scopo è quello della protezione dai contenuti "illegali e nocivi", traduzione letterale della formula originaria americana *illegal and harmful*. Si dovrebbe partire da questa definizione per stabilire le regole. Ma non ci si accorge, o si finge di non accorgersi, che in questa formulazione c'è già un concetto di censura. Perché non c'è dubbio su che cosa si intende per "illegale" (ciò che è contrario alla legge), ma chi stabilisce che cosa è "nocivo"? Inoltre la congiunzione *and* lega in un solo fascio i reati e altre informazioni di contenuto discutibile. Il che mi sembra difficile da accettare.
Facciamo un esempio: la pedofilia è illegale in tutti i paesi civili. Compiere atti sessuali su bambini è un reato dovunque questo comportamento sia previsto come tale. Ma la diffusione di immagini di contenuto erotico è reato olo in alcune nazioni, mentre è generalmente riconosciuto che alcuni tipi di rappresentazioni erotiche possono avere effetti negativi su determinati soggetti: basta questo per definire "nocive" tutte le rappresentazioni erotiche? Se invece si intendono come nocive solo le rappresentazioni erotiche che superano certi limiti, chi stabilisce questi limiti? Ecco come riappare lo spettro della censura!
A ben guardare, quando si afferma che l'autoregolamentazione deve essere adottata per evitare la diffusione di contenuti illegali e nocivi, si pone il problema in termini limitativi e fuorvianti. Il fine delle norme deve essere la protezione del "cittadino telematico" in quanto tale, e quindi *anche, e non solo*, la sua difesa contro i contenuti illegali, o che possono costituire un rischio per determinate categorie di soggetti. E quindi, posto che l'autoregolamentazione deve essere adottata dai fornitori di servizi, le norme devono essere poste in primo luogo a difesa dei diritti degli utenti. I quali utenti devono poter scegliere tra tutti i contenuti che non siano in contrasto con la legge. Quindi, eliminati in qualche modo all'origine i contenuti illegali, è necessario stabilire procedure per la selezione dei contenuti che *possono essere nocivi*, in breve dei contenuti "pericolosi".
Per questo motivo, la bozza di codice di autoregolamentazione pubblicata in queste pagine usa la formula "contenuti illegali o pericolosi" al posto dell'espressione usuale "contenuti illegali e nocivi". La differenza è sostanziale.
C'è poi l'aspetto, tutt'altro che secondario, della

d) ACCCESS PROVIDER (AP): chiunque offre al pubblico l'accesso ad una rete telematica, l'utilizzo delle eventuali funzioni, nonché lo spazio fisico necessario all'utilizzo di queste ultime.
e) SERVICE PROVIDER (SP): chiunque offre al pubblico servizi di telecomunicazioni.
f) CONTENT PROVIDER (CP): chiunque, come attività professionale o comunque continua o abituale, immette nella rete informazioni di qualsiasi tipo.
g) UTENTE: il destinatario dell'attività esercitata dai soggetti di cui alle lettere c), d), e) ed f) del presente comma, sia esso una persona fisica, giuridica, ente, associazione o società commerciale.

Titolo II - Regole di comportamento

5. Procedure di controllo degli accessi
Gli aderenti per quanto di loro competenza e nel rispetto delle leggi vigenti adottano le seguenti procedure:
a) Identificazione certa dell'utente titolare di un abbonamento al proprio sistema.
b) Registrazione automatica (LOG) dei collegamenti compiuti dall'utente, al fine di documentare eventuali commissioni di atti illeciti e controllo automatico e registrazione delle attività che, sul piano tecnico, siano potenzialmente idonee a causare danni o commettere atti illeciti.

6. Dati personali
Gli aderenti mantengono la massima riservatezza sulle informazioni personali degli utenti, delle quali venissero a conoscenza in seguito all'esecuzione del contratto di abbonamento.
Gli aderenti hanno la facoltà di concedere l'accesso anonimo all'utente preventivamente identificato, rivelandone la reale identità solo a fronte di un provvedimento dell'autorità giudiziaria.

7. Adozione di misure di sicurezza
Gli aderenti adottano sui propri sistemi le misure di sicurezza logica e fisica previste dalle leggi e dai regolamenti e ne informano gli utenti.

8. Uso di sistemi crittografici e certificazione delle chiavi
Gli aderenti adottano un sistema di attribuzione e certificazione delle chiavi crittografiche fornite agli utenti dietro loro specifica richiesta.

9. Modalità di tenuta dei log
Gli aderenti conservano i log delle connessioni in supporti non alterabili per la durata minima di un anno.

10. Informazioni agli utenti
Gli aderenti informano gli utenti preventivamente e in modo chiaro:
a) dei termini e delle condizioni di abbonamento;
b) delle modalità di fruizione delle funzioni e dei servizi, compresi i termini di conservazione delle informazioni;
c) delle possibilità di accesso a contenuti pericolosi e delle procedure di selezione dei medesimi;
d) delle responsabilità derivanti dall'immissione, da parte degli stessi utenti, di contenuti pericolo-

Le fonti di riferimento

La bozza di codice di autoregolamentazione pubblicata in queste pagine è stata preparata sulla base dell'attuale contesto legislativo europeo e italiano, con particolare attenzione alla vigente normativa specifica:

1. **direttiva 90/388/CEE del 28 giugno 1990** - Relativa alla concorrenza nei mercati dei servizi di telecomunicazioni - e successive aggiunte;
2. **decreto legislativo 29 dicembre 1992 n. 518** - Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore;
3. **legge 23 dicembre 1993 n. 547** - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
4. **decreto legislativo 17 marzo 1995 n. 103** - Recepimento della direttiva 90/388/CEE relativa alla concorrenza nei mercati dei servizi di telecomunicazioni – e decreti applicativi;
5. **legge 31 dicembre 1996 n. 675** - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
6. **legge 31 dicembre 1996 n. 676** - Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Due disegni di legge in discussione al Senato contengono alcuni riferimenti all'oggetto di questo studio, peraltro assai vaghi:

7. **disegno di legge S1021** - Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sul sistema radiotelevisivo;
8. **disegno di legge S1138** - Disciplina del sistema delle telecomunicazioni.

Per la definizione del codice di autoregolamentazione dei fornitori di servizi telematici è molto importante il dibattito in corso a livello mondiale sulle "regole di Internet", dibattito che in parte riguarda le normative nazionali e internazionali, in parte i codici di autoregolamentazione. Per la stesura della bozza di Codice di autoregolamentazione sono stati considerati i documenti più rilevanti prodotti negli ultimi tempi. Ecco i più interessanti:

9. per quanto riguarda gli USA, dove il dibattito sulla regolamentazione del ciberspazio ha prodotto un'enorme quantità di documenti, vanno considerati diversi spunti nel quadro sistematico sullo stato della ricerca offerto dalla **Cybersquirrel**, alla URL http://www.cybersquirrel.com/clc/clcindex.html;
10. una documentazione giuridica sistematica sulle telecomunicazioni è presente anche nel sito della **Cornell University** (http://www.law.cornell.edu/topical.html);
11. importanti riferimenti si trovano nel sito della **Electronic Frontier Foundation** (http://www.eff.org), che offre un panorama completo del dibattito sulla regolamentazione del ciberspazio a livello mondiale;
12. sempre con riferimento al dibattito negli USA, va considerata la decisione del 12 giugno '96 della **Corte federale della Pennsylvania** nella causa promossa dalla American Civil Liberties Union e altri contro il "Communication Decency Act" inserito nel "Telecommunications Act of 1996" (il documento, reperibile su Internet alla URL http://www.complaw.com/lawlibrary/cda.html contiene importanti definizioni della natura di Internet e delle ragioni della libertà di espressione che la caratterizza; il testo del Telecommunications Act è disponibile nell'edizione ufficiale alla URL http://www.chron.com/content/interactive/special/freespeech/bill.html);
13. i documenti dell'**Unione europea** sulle "Informazioni di contenuto illegale e nocivo su Internet" (in particolare la "Comunicazione del sig. Bangemann alla Commissione"), alla URL http://www2.echo.lu/legal/internet.html, costituiscono il punto di riferimento imprescindibile per la regolamentazione in Italia, insieme alla "Resolution adopted at the Telecommunications Council of 28 November 1996", sempre sul sito della DG XIII della UE alla URL http://www2.echo.lu/legal/en/internet/content/resol.html;
14. considerazioni interessanti sulla politica inglese per la società dell'informazione sono in uno studio di Stephen Saxby, **A UK national information policy for the electronic age**, alla URL http://www2.echo.lu/legal/en/access/saxby/ch4/ch4.html, che considera il British Telecommunications Act 1981 e il Telecommunications Act 1984;
15. in Francia è stato presentato, il 27 gennaio scorso, un codice di regolamentazione di impostazione piuttosto repressiva, che suscita accese polemiche.

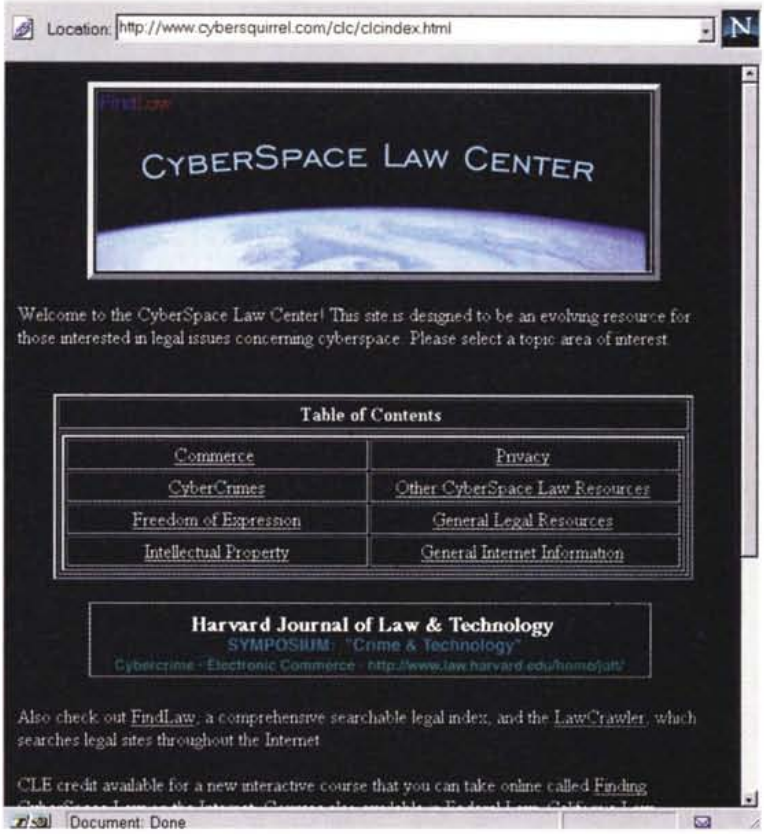
Per quanto riguarda il nostro paese, deve essere considerato in primo luogo il dibattito che si svolge dalla primavera del '95 in questo Forum. I documenti più interessanti sono:

16. **Ipotesi di codice di autodisciplina per la comunicazione telematica** di Giuseppe Corasaniti - 31.05.95 (http://www.mclink.it/inforum/corasan1.htm);
17. **Sicurezza dei sistemi informativi e responsabilità dell'operatore di sistema** di Gianni Buonomo - 13.06.95 (http://www.mclink.it/inforum/buonomo.htm);
18. **Esplorando il ciberspazio con le lenti del giurista - Prime note di un gruppo di "cibernauti-giuristi" guidati da Costantino Ciampi** - 18.06.95 (http://www.mclink.it/inforum/ciampi.htm) - con gli studi **Diritti di libertà sulle "autostrade digitali"** di Maria Antonietta Laura Mazzola e Rosanna Ortu e **Reti telematiche e propaganda. Tra libertà di manifestazione del pensiero e tutela dell'individuo** di Francesca Angelini e Sebastiano Faro;
19. **Le difficili regole della tecnologia informatica** di Giuseppe Corasaniti - 26.06.95 (http://www.mclink.it/inforum/corasan2.htm);
20. **La responsabilità del gestore del sistema informatico per omessa adozione di misure di sicurezza** di Gianni Buonomo - 29.01.96 (http://www.mclink.it/inforum/buonomo3.htm);
21. **Il decreto legislativo 103/95 e gli Internet Service Provider** di Manlio Cammarata e Andrea Monti - 22.02.96 (http://www.mclink.it/inforum/103def.htm);
22. **Aspetti problematici del regime giuspubblicistico di Internet** di Pasquale Costanzo - 14.10.96 (http://www.mclink.it/inforum/costanzo.htm)
23. **Data Protection e Telecomunicazioni** di Giovanni Maria Borrello - 05.12.96 (http://www.mclink.it/inforum/borrell2.htm);
24. **Il dibattito sulla regolamentazione di Internet** nell'area "Tesi e ricerche" (http://www.mclink.it/inforum/tesi/indicaz2.htm#I_INTERNET_CONTENTS), con una serie di collegamenti ad altri documenti reperibili sulla Rete o in questo stesso Forum Multimediale.
25. **Banche dati, privacy e sicurezza: gli obblighi del gestore** di Gianni Buonomo - 28.01.97 (http://www.mclink.it/inforum/buonomo4.htm);
26. **Aspetti evolutivi del regime giuridico di Internet** di Pasquale Costanzo - 28.01.97 (http://www.mclink.it/inforum/costanz2.htm);
27. **La legge 675/96 vieta Internet?** di Manlio Cammarata - 18.02.97 (http://www.mclink.it/inforum/cammar4.htm).
28. E' stato inoltre tenuto presente il **Codice di autodisciplina pubblicitaria**, che rappresenta il primo esempio in Italia di autoregolamentazione efficace nei rapporti tra mondo della produzione e cittadini-consumatori.

protezione dell'utente per quanto riguarda il servizio in sé: informazione completa e comprensibile sulle tariffe e sulle caratteristiche del servizio, sui diritti e i doveri dell'abbonato, sulle procedure di sicurezza, di protezione dei dati personali e di selezione dei contenuti. Il codice di autoregolamentazione deve tradursi in precise clausole del contratto di abbonamento, la cui accettazione rende l'utente soggetto attivo della comunità telematica e quindi vincolato alle sue regole.

La selezione dei contenuti

Il "Rapporto alla Commissione Europea", che si può leggere (anche in italiano) alla URL http://www2.echo.lu/legal/internet.html, presenta un quadro esauriente e abbastanza equilibrato dello sviluppo di Internet e dei suoi problemi, sempre con la riserva espressa nel precedente paragrafo, di un'ottica più repressiva di quanto il tono lasci intendere. Per risolvere il problema dei contenuti "nocivi" il documento accoglie in pieno la proposta di adottare un meccanismo di filtri che consenta una selezione dei contenuti da parte dell'utente, sulla base di "contrassegni" apposti dai fornitori di informazioni. Sono già in uso diversi sistemi di questo tipo; quello che sembra abbia le maggiori possibilità di affermarsi a breve termine come standard è il PICS (Platform for Internet Content



Un panorama completo della legislazione in materia di telematica è disponibile alla URL http://www.cybersquirrel.com/clc/clcindex.html.

si, offensivi o comunque in contrasto con le disposizioni vigenti.

11. Contenuto pubblicitario dei servizi
Gli aderenti strutturano i servizi offerti in modo che gli annunci pubblicitari non costituiscano aggravio rilevante per gli utenti, per via dei maggiori tempi di connessione o per altro motivo.

12. Utilizzo dei sistemi di messaggistica
Gli aderenti limitano per quanto possibile e per quanto di loro competenza l'invio di messaggi non richiesti, a meno che ciò non sia necessario per esigenze operative.

13. Contenuti illegali o pericolosi
Fatte salve le disposizioni dell'art. 10, lettera d), gli aderenti possono ospitare, a proprio insindacabile giudizio, qualsiasi tipo di materiale, purché legittimo, a condizione che siano rispettate, in quanto possibile, le disposizioni del successivo art. 14.

14. Classificazione dei contenuti
Gli aderenti adottano sistemi standard di classificazione e selezione dei contenuti illegali o nocivi, informando gli utenti delle possibilità di filtraggio, e forniscono, se richiesti, l'assistenza per l'installazione da parte dell'utente dei sistemi di selezione dei contenuti.
E' facoltà degli aderenti offrire al pubblico accessi limitati con i sistemi di classificazione adottati in sede internazionale.

15. Controllo dei contenuti
Stante l'impossibilità tecnica di controllo preventivo dei contenuti immessi da terzi, gli aderenti rimuovono i contenuti palesemente illegali o offensivi, o che non rispettano le disposizioni degli articoli 14 e 15, non appena ne vengono a conoscenza.

16. Adesione al codice di autodisciplina pubblicitaria
Relativamente all'attività pubblicitaria gli aderenti si conformano a quanto stabilito dal codice di autodisciplina pubblicitaria, in quanto applicabile.

17. Indicazione espressa del responsabile
Gli aderenti informano l'utente che negli spazi da quest'ultimo gestiti devono sempre essere chiaramente indicati almeno il nome del responsabile e il suo recapito telematico.

18. Utilizzo degli spazi
Gli aderenti possono, secondo il proprio insindacabile giudizio, ospitare sui propri spazi qualsiasi tipo di materiale purché legittimo a condizione che:
a) sia identificato in modo inequivoco l'utente dello spazio
b) l'utente sia stato preventivamente informato delle procedure di gestione dello spazio suddetto
c) l'utente renda accessibile a terzi il materiale critico solo dopo aver acquisito la ragionevole certezza circa l'età dei terzi e comunque non

Selection), del quale abbiamo parlato nel numero 167. Questo meccanismo è già stato adottato dai più grandi fornitori di informazioni, come CompuServe, America On Line e Prodigy, e dalle case che producono i browser, come Microsoft e Netscape (informazioni complete alla URL http://www.w3.org/pub/WWW/PICS).
Il meccanismo si fonda su un certo numero di etichette (tag) da inserire nelle singole pagine per indicare il tipo di contenuto, secondo una classificazione standard. Il programma di navigazione può essere programmato per rifiutare i contenuti contraddistinti da determinati tag, oppure per lanciare un avvertimento all'utente nel caso che la pagina richiesta appartenga a una certa categoria. Naturalmente l'elenco dei tag "proibiti" o "sconsigliati" può essere protetto da una password, il che consente ai genitori (o agli insegnanti, nel caso di impieghi scolastici) di stabilire a quali contenuti i ragazzi non possono accedere. C'è da notare che all'inizio questo sistema è stato studiato per limitare gli utilizzi "ludici" di Internet in ambito aziendale e che sulle prime è stato accolto come una forma di censura. Ma non è vero: se un'azienda spende una certa quantità di soldi per fornire uno strumento di lavoro ai suoi dipendenti, ha il diritto di impedirne un uso improprio. Lo stesso discorso vale per qualsiasi organizzazione che metta a disposizione di terzi un accesso alla Rete. Tra parentesi, è successo in Italia alcuni mesi fa, quando si è gridato alla censura e alla repressione della libertà per la chiusura di una pagina gestita dagli studenti su un sito universitario, pagina che conteneva espressioni giudicate ingiuriose. Ebbene, se lo Stato spende dei soldi, attraverso l'istituzione accademica, per dare agli studenti uno strumento utile per lo studio, ha il diritto di vietare che ne venga fatto un uso diverso. In verità si tratta di vedere se sia o no opportuno che le istituzioni pubbliche mettano gratis a disposizione dei cittadini anche spazi "liberi" di discussione. Fermo restando che su questi spazi sarebbe comunque vietato offendere il prossimo o compiere atti illeciti, il problema è politico, e quindi estraneo a queste pagine. Ma comunque merita una discussione nelle sedi appropriate.
Chiusa la parentesi, torniamo al PICS e alla selezione automatica dei contenuti. Non è certo una panacea che possa guarire tutti "i mali di Internet" e assicurare una sana crescita psicologica dei minori. Non spetta a un software educare i ragazzi, è compito della famiglia e della scuola. D'altra parte, se un genitore si disinteressa di come crescono i suoi figli, non si preoccupa certo di installare o far installare il filtro sul PC di casa! La selezione automatica dei contenuti è solo un aiuto per chi ha già deciso di affrontare questo tipo di questioni. A questo proposito c'è da segnalare una possibilità

rendendo immediatamente visibile o accessibile detto materiale senza il filtro previsto dall'art. 14.

Titolo IV - Organi e competenza

19. Commissione di controllo
La commissione di controllo è l'organo che decide, sulla base di quanto stabilito nel presente codice, dei ricorsi e delle segnalazioni relative a quanto di competenza del presente codice.

20. Composizione e caratteristiche
La commissione di controllo è costituita da tre membri effettivi e da due membri supplenti.
I membri della commissione sono scelti fra soggetti che abbiano una comprovata ed inequivocabile esperienza e competenza professionale nei settori della comunicazione e delle tecnologie.
Almeno uno dei membri effettivi deve essere un avvocato o un docente universitario esperto di diritto delle tecnologie.
La commissione decide nella più totale autonomia e nell'interesse generale.
I membri effettivi e supplenti della commissione di controllo durano in carica due anni e possono essere nominati consecutivamente per una sola volta.
I membri vengono nominati dagli aderenti al presente codice.

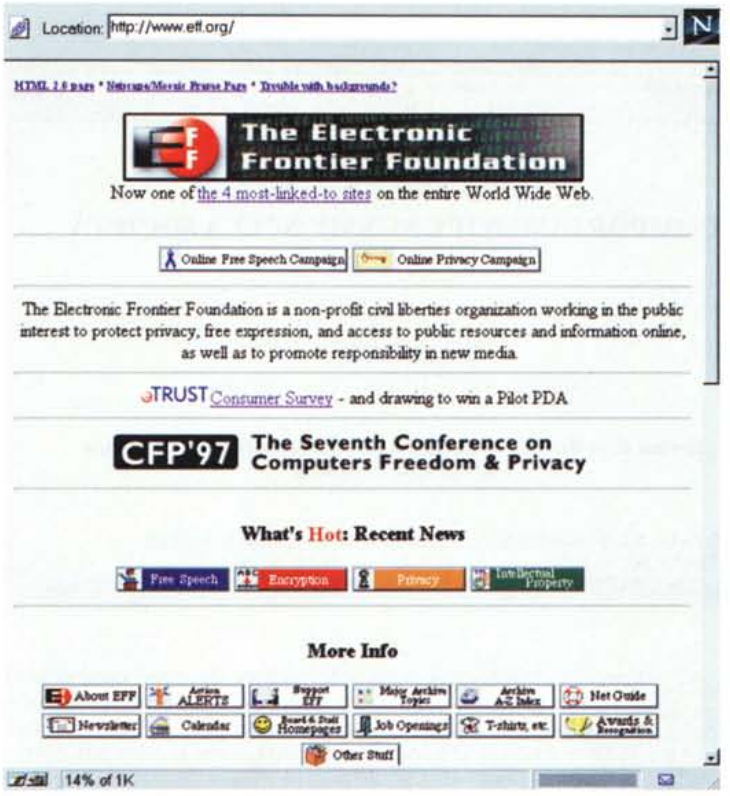
Titolo V - Procedure contenziose

21. Segnalazioni
Chiunque e con qualsiasi mezzo può segnalare alla commissione di controllo violazioni di quanto previsto nel presente codice.
Le segnalazioni anonime non vengono prese in considerazione.

22. Istruzione preventiva
Se la commissione ritiene infondata la segnalazione ne dà comunicazione all'autore della segnalazione senza obbligo di motivare.
Se la commissione ritiene che la segnalazione ricevuta non sia infondata invita l'aderente a fornire chiarimenti.
Se i chiarimenti sono ritenuti sufficienti la commissione non procede con l'instaurazione di un procedimento formale e comunica il tutto all'autore della segnalazione, motivando adeguatamente nei limiti in cui ciò non costituisca violazione di segreto industriale o professionale o aziendale.

23. Attivazione della procedura
Se la commissione non ritiene di dover procedere ai sensi dell'articolo precedente, invia all'aderente un piego raccomandato contenente le contestazioni e la data entro la quale devono pervenire alla commissione delle note difensive.

(che potrebbe costituire anche un'opportunità commerciale per gli Internet provider): un sistema di selezione automatica dei contenuti "pericolosi" può essere installato anche a livello di "server" e di conseguenza si possono offrire al pubblico accessi "puliti". Come è già stato fatto negli USA, un provider può offrire due tipi di abbonamento, che fanno capo a diverse linee telefoniche: uno "completo" e uno "filtrato" a protezione dei minori.
Resta da dire che il PICS, o altri sistemi analoghi, funzionano solo se sono adottati da tutti i fornitori di contenuti. E qui torniamo all'autoregolamentazione: i fornitori di accessi, una volta che il sistema sia diventato standard o comunque abbastanza diffuso, devono impegnarsi a non consentire il collegamento ai fornitori di contenuti che non rispettino le regole. Questi sarebbero costretti a uniformarsi per non essere tagliati fuori dalla Rete. Naturalmente l'uso di etichette improprie, tali da trarre in inganno i programmi di selezione, dovrebbe essere considerato illecito (e già oggi, in qualche caso, potrebbe essere un reato).



Il sito della Electronic Frontier Foundation (http://www.eff.org) è il punto di riferimento obbligato per tutti i dibattiti sulla regolamentazione di Internet.

Le finalità del codice

Vediamo ora più in dettaglio quali possono essere le principali regole del codice di autoregolamentazione di Internet in Italia, contenute nella bozza

L'aderente può chiedere in qualsiasi momento di essere ascoltato personalmente.
Acquisiti gli elementi necessari alla decisione la commissione emana la propria decisione motivata, fissando all'uopo una data che deve essere comunicata alle parti. Ricevuta la comunicazione della data le parti non possono più modificare le proprie richieste né produrre altro materiale probatorio.
L'intero procedimento deve concludersi entro sei mesi dall'attivazione della procedura.

24. Consulenze tecniche
La commissione procede all'acquisizione delle informazioni necessarie alla decisione, anche ricorrendo all'ausilio di consulenze tecniche.
Dell'eventuale consulenza tecnica è data notizia anche all'autore della segnalazione che, sostenendone i costi, può intervenire in proprio se qualificato tecnicamente, o a mezzo di un proprio consulente.

25. Documentazione della procedura
Di ogni procedura devono essere conservati gli atti e i verbali preferibilmente in formato digitale al fine di consentire l'eventuale verifica dell'operato della commissione.
I provvedimenti della commissione vengono diffusi in rete su un sito appositamente istituito.

26. Riesame
Entro trenta giorni dalla comunicazione della decisione l'aderente può chiedere il riesame della decisione.
In questo caso la decisione è adottata dai due membri supplenti e da uno dei tre membri effettivi estratto a sorte.
Il procedimento di riesame deve concludersi entro tre mesi.

27. Altre controversie
Se la segnalazione non riguarda fatti previsti dal presente codice o se non è possibile attivare la procedura, viene incardinato un arbitrato. Ognuna delle parti nomina un arbitro e il terzo viene nominato dal Presidente del Tribunale della sede legale dell'aderente.

Titolo VI - Sanzioni

28. Violazione delle regole di comportamento
Se viene riscontrata la violazione di una delle regole di comportamento la commissione ne impone con effetto immediato l'adozione.

29. Spese della procedura
In caso di accertata violazione di quanto previsto dal codice, l'aderente deve farsi carico delle spese di procedura, salvo che non sia diversamente stabilito con adeguata motivazione.
Le spese devono essere documentate.
Le spese non documentabili o non documentate non vengono prese in considerazione.
In quanto applicabile, vige la tariffa prevista per le attività stragiudiziali degli avvocati.


Location: http://www.mclink.it/inforum/corasan1.htm

FORUM MULTIMEDIALE
LA SOCIETÀ DELL'INFORMAZIONE

COMPORTAMENTI E NORME NELLA SOCIETÀ VULNERABILE

INTERVENTI - 4

Ipotesi di codice di autodisciplina per la comunicazione telematica
di Giuseppe Corasaniti

1. LIBERTA', RESPONSABILITA', SICUREZZA DELLA COMUNICAZIONE TELEMATICA

Document: Done

Nel Forum multimediale "La società dell'informazione" (http://www.mclink.it/inforum) la discussione sull'autoregolamentazione di Internet è incominciata due anni fa, con questo intervento di Giuseppe Corasaniti.

pubblicata in queste pagine. Si deve premettere che la bozza è stata preparata come normativa specifica per i servizi in ambito telematico (Internet, BBS, banche dati on-line) e non per tutti i servizi che sfruttano le nuove tecnologie, come Videotel, Audiotel e simili. Anche se ci sono forti analogie tra i due settori, e molte regole possono essere comuni, le modalità di accesso e le dimensioni che il settore telematico ha assunto, e che assumerà nel prossimo futuro, rendono difficilmente applicabili le forme di controllo specifico che si possono istituire per i servizi "telefonici".
Il codice di autodisciplina dei fornitori di servizi telematici deve regolare i rapporti tra tutti i soggetti interessati, assicurando il rispetto delle leggi e dettando norme adeguate per le situazioni non previste o non ancora regolate dall'ordinamento giuridico. Deve rendere trasparente il rapporto tra gli abbonati e gli Internet provider e assicurare a questi ultimi un quadro di certezza normativa che ne favorisca l'attività. Esso deve quindi operare su due versanti: da una parte il rapporto tra provider e abbonato e dall'altra quello tra provider e organismi pubblici.
Il codice deve avere come presupposto il valore delle attività telematiche e come fine il loro sviluppo e la protezione dei diritti dei consumatori e dei fornitori. Deve avere obiettivi di sviluppo e non di repressione. La repressione dei contenuti illegali e il controllo o la selezione dei contenuti pericolosi devono essere inseriti in un quadro complessivo di definizione dei diritti e dei doveri di tutti i soggetti coinvolti nelle attività telematiche. E' opportuno quindi vedere le regole sotto due diversi punti di vista: il rapporto tra utenti e provider e l'attività di questi ultimi nel contesto del diritto vigente.
Sul primo punto va osservato che la maggioranza degli utenti di Internet non è più costituita da "addetti ai lavori", ma da gente comune, anche se ancora di livello socio-culturale alto o medio-alto. Si tratta quindi di "consumatori" a tutti gli effetti. Il rapporto tra i gestori dei sistemi e gli utenti è una relazione tra produttore (o distributore) e consumatore. Dunque il codice ha in primo luogo lo scopo di assicurare al consumatore il più ampio sfruttamento delle possibilità delle Rete, tutelando la sua posizione di "parte debole" nei confronti del fornitore e proteggendolo contro i rischi che possono derivare da un uso non abbastanza consapevole di Internet. Di conseguenza deve vincolare i fornitori sui seguenti punti:
1. chiarezza delle condizioni generali e particolari dei contratti di abbonamento;
2. informazione chiara e completa sull'uso del sistema, con particolare attenzione ai problemi della sicurezza e alla gestione delle password;
3. sicurezza delle transazioni e riservatezza della corrispondenza, con l'applicazione dei sistemi di protezione più efficaci adottati a livello internazionale;
4. protezione degli utenti contro azioni illecite, come frodi commerciali, violazioni della riservatezza, diffamazioni e così via;
5. protezione dai contenuti illeciti o offensivi della dignità delle persone o della morale, con l'adozione dei sistemi di selezione dei contenuti a mano a mano che essi vengono accettati e applicati sulla Rete;
6. protezione dell'eventuale richiesta di anonimato dell'utente, e comunque dei suoi dati personali, rispettando nel contempo le esigenze di sicurezza della Rete e di collaborazione con le forze dell'ordine e la magistratura nei procedimenti giudiziari.
E' comunque necessario distinguere tra gli obblighi che fanno capo ai fornitori di accessi e quelli che devono essere assolti dai fornitori di contenuti.

L'Internet provider e le norme di legge

Vediamo ora l'altro aspetto del codice di autoregolamentazione, quello che deve assicurare che l'attività dei fornitori di accessi e di servizi possa svolgersi in un quadro di regole certe, che chiariscano diritti e doveri, con soluzioni comuni che rendano agevole l'applicazione delle norme civili, penali e amministrative.
Il Codice di autoregolamentazione deve quindi prevedere:
1. modi e regole comuni per l'applicazione delle disposizioni di legge e regolamentari;
2. norme comuni per l'identificazione degli abbonati, assicurando la protezione dei dati personali;
3. i limiti minimi e massimi delle informazioni sull'attività degli abbonati, registrate automaticamente (LOG), modi e durata della conservazione dei log, anche in funzione di eventuali richieste dell'autorità giudiziaria (per questa materia sarebbe opportuna l'emanazione di precise norme di legge, secondo la previsione della legge-delega 676/96 per la protezione dei dati personali);

4. le forme di collaborazione con l'autorità giudiziaria nel caso di indagini penali;
5. la creazione di organismi collegiali che controllino e incoraggino l'applicazione del Codice di autoregolamentazione e sanzionino i comportamenti contrari al Codice stesso.

Ma tutto questo non è sufficiente, se manca un sistema organico di norme di legge che regolino le attività telematiche nella parte che coinvolge esigenze superiori, come il diritto all'informazione, la repressione dei reati, il disegno generale del sistema delle telecomunicazioni.

Si aggiunga che alcune norme contenute nella bozza del codice di autodisciplina possono essere in contrasto con il diritto vigente, in particolare per quanto attiene alla responsabilità civile e penale dei fornitori di servizi. Non si tratta, sia chiaro, di proposte "sovversive"; il fatto è che ci troviamo di fronte a nuove situazioni, che richiedono regole nuove. Il legislatore deve quindi provvedere con urgenza a:

1. stabilire norme di limitazione o esenzione della responsabilità per i contenuti che il fornitore non può controllare prima della pubblicazione, salva la

facoltà di rimuoverli, a suo insindacabile giudizio, quando abbia fondati sospetti di illiceità del materiale pubblicato, e salvo l'obbligo di rimuoverlo su richiesta della persona offesa o su segnalazione motivata di terzi. La limitazione o l'esenzione della responsabilità può essere riconosciuta in due casi:
a) quando le informazioni provengano da altri fornitori;
b) quando il fornitore abbia adottato le precauzioni indicate dal codice di autoregolamentazione, in particolare l'identificazione dell'utente;
2. definire i requisiti sulla base dei quali un sito deve essere registrato come testata giornalistica (indispensabile per l'applicazione dell'art. 25 della 675/96);
3. introdurre una modifica all'attuale normativa sulla stampa, che stabilisca che i direttori responsabili delle testate giornalistiche telematiche registrate ai sensi della legge 47/48 sono responsabili solo dei contenuti redazionali e di tutti i contenuti per i quali non sia espressamente indicato il nome dell'autore, il quale se ne assume contrattualmente la responsabilità secondo le previsioni del codice di autoregolamentazione;
4. modificare la normativa sulla stampa anche per quanto riguarda l'obbligo del deposito di copie della pubblicazione presso gli apposti uffici: è semplicemente impossibile, e d'altra parte si tratta, sotto alcuni aspetti, di una criticabile "norma di polizia".
Resta da risolvere un altro problema, forse il più grave e il più difficile posto dalle esigenze di regolamentazione delle attività telematiche: qualsiasi norma nazionale può essere facilmente aggirata, grazie alla globalità della Rete. Sono necessari accordi internazionali che portino a una legislazione il più possibile uniforme nei diversi paesi. Anzi, sarebbe necessaria una legislazione comune, transnazionale, perché transnazionale è di fatto il mondo delle telecomunicazioni.
Il discorso è complesso e va affrontato a parte. Qui mi limito ad avanzare l'ipotesi che il solo modo di regolamentare la Rete sia un sistema di norme speciali, frutto di accordi internazionali, che considerino il sistema delle telecomunicazioni come una sorta di territorio a sé stante, di volta in volta sovrapposto ai territori nazionali. O, meglio, come un meta-territorio, le cui norme interagiscano e siano accolte nei diversi sistemi legislativi come norme di diritto internazionale. E' una strada lunga e difficile da percorrere, ma forse è la sola possibile per favorire il corretto sviluppo della società dell'informazione globale.

La responsabilità del provider

La responsabilità civile e penale del provider è uno degli aspetti più delicati della regolamentazione delle attività telematiche.
Attraverso un sistema telematico possono essere compiuti diversi atti illeciti. Alcuni di rilevanza penale, cioè reati, altri soltanto civili, cioè che possono dar luogo a un risarcimento del danneggiato. Facciamo l'esempio di un reato previsto dalla legge 547/93, come l'introduzione abusiva in un sistema protetto da misure di sicurezza, compiuta da un utente sconosciuto. La persona offesa sporge querela, provando che la violazione è partita da un certo sistema. Il gestore di questo non può essere imputato del reato (a meno che non si provi che è stato lui!) perché la responsabilità penale è personale (art. 27 della Costituzione). Però potrebbe essere accusato di favoreggiamento, se non fornisce all'autorità giudiziaria tutte le informazioni in suo possesso per l'identificazione del responsabile, e potrebbe anche essere tenuto al risarcimento del danno (responsabilità civile) se la vittima prova che non sono state prese tutte le misure necessarie a evitare che si compisse un atto illecito prevedibile.
Quando un sito telematico è registrato come testata giornalistica è possibile anche una forma di responsabilità penale del direttore, per il reato di "omesso controllo" (art. 57 del codice penale, ne abbiamo parlato sul n. 169). Ma sappiamo che il responsabile di una pubblicazione telematica non può materialmente controllare i milioni di informazioni che possono passare per il suo sistema, perché sono messe in rete da altri in tempo reale (si può discutere se la previsione dell'art. 57 valga anche per l'informazione telematica e non solo per quella stampata, ma il problema resta). Come se ne esce?
La prima precauzione che deve essere presa riguarda l'identificazione degli abbonati e la documentazione del traffico, con i cosiddetti "log". Il provider deve essere in grado, almeno entro certi limiti, di fornire all'autorità giudiziaria tutti gli elementi utili all'identificazione del responsabile di un atto illecito. Nel caso che l'azione o l'informazione illegale provenga dalla rete, deve poter indicare il sito dal quale essa è arrivata. Se dai log risulta che il responsabile (apparente, perché l'autore dell'illecito potrebbe aver usato una password rubata) è un suo abbonato, deve comunicarne le generalità.
Ma un punto deve essere chiaro: è necessario stabilire che il provider non è responsabile di quello che non può materialmente controllare. Sembra ovvio (*ad impossibilia nemo tenetur*; nessuno è obbligato all'impossibile), ma nell'attuale quadro legislativo non lo è. In particolare, la formulazione della legge 675/96 sulla protezione dei dati personali pone a carico del "titolare del trattamento", di fatto il legale rappresentante della struttura telematica, una responsabilità che non sembra facilmente circoscrivibile.
La bozza di codice di autoregolamentazione pubblicata in queste pagine definisce i limiti della responsabilità del provider per i contenuti del sito, ma l'efficacia di queste previsioni è subordinata a una modifica del quadro legislativo vigente, soprattutto per quanto riguarda il controllo del direttore responsabile della testata telematica e la protezione dei dati personali. Occorre anche rivedere le norme di procedura penale sulle indagini in materia di reati telematici.